Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/GB05/001237

International filing date: 30 March 2005 (30.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: GB
Number: 0407335.9
Filing date: 31 March 2004 (31.03.2004)

Date of receipt at the International Bureau: 09 May 2005 (09.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/GB2005/001237.

PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
The Patent Office

INVESTOR IN PEOPLE

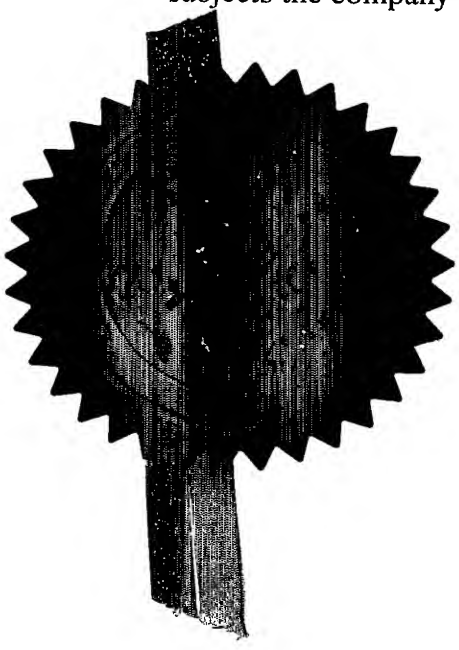
The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed

Dated 21 April 2005

P[redacted]orm 1/77

THE PATENT OFFICE
A
31 MAR 2004
LONDON

The Patent Office

1/77

01APR04 E885537-1 D03052
P01/7700 0.00-0407335.9 ACCOUNT CHA

Patents Act 1977
(Rule 16)

The Patent Office
Cardiff Road
Newport
Gwent NP10 8QQ

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

1. Your reference

A30354

2. Patent application number
(The Patent Office will fill in this part)

31 MAR 2004

0407335.9

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

BRITISH TELECOMMUNICATIONS public limited company
81 NEWGATE STREET
LONDON, EC1A 7AJ, England
Registered in England: 1800000

Patents ADP number *(if you know it)*

~~1867002~~ 6300388001

If the applicant is a corporate body, give the country/state of its incorporation

UNITED KINGDOM

4. Title of the invention

AUTHORISATION

5. Name of your agent *(if you have one)*

"Address for Service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

BT GROUP LEGAL
INTELLECTUAL PROPERTY DEPARTMENT
PP: C5A, BT CENTRE
81 NEWGATE STREET
LONDON, EC1A 7AJ, ENGLAND

Patents ADP number *(if you know it)*

~~1867001~~ 8772378001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day/month/year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.

(See note (d))

YES

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	-
Description	- **08**
Claim(s)	- **03** CF
Abstract	- **01**
Drawing(s)	- **03** +3

10. If you are also filing any of the following, state how may against each item

Priority Documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	- **ONE**
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature(s) Date:

31 March 2004

CHABASSEUR, Vincent Robert, Authorised Signatory

12. Name and daytime telephone number of person to contact in the United Kingdom

Mark WATSON **020 7356 6163**

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

Authorisation

The present invention relates to authorisation, in particular to authorisation using a digital certificate.

It is know to use digital certificates to authorise a node or a user, for example to authorise the node or user access to data or services. Such certificates normally have a digital signature which is encrypted using a public key cryptography system. The digital signature is normally a function of the characters forming the message content of the certificate, such that a recipient can perform a function on the signature in order to determine with some degree of certainty that a received certificate has not been altered.

According to one aspect of the invention, there is provided a method of authorising data transfer to a mobile node, the method including the steps of: receiving a digital certificate from the mobile node, the digital certificate including a message body, a digital signature for verifying the content of the message body, and, geographical information derived from a physical location; performing a comparison between the geographical information of the certificate and a further item of geographical information; and, making an authorisation decision in dependence on the result of the comparison.

Further aspects of the invention, including a method of generating a digital certificate, are provided as specified in the appended claims.

The present invention is described in further detail below, by way of example, with reference to the following drawings in which:

Figure 1 shows a network system according to the present invention;

Figure 2 is a schematic representation of a digital certificate;

Figure 3 is a schematic representation of message flows between nodes;

Figure 4 shows the transfer of messages involved in the creation of a security association; and,

Figure 5 is a more detailed exampled of a certificate.

In Figure 1, there is shown a network system 10 having a main network 12 and at least one mobile node 14. The main network, which is preferably static, has a plurality of nodes 16 connected by links 18. Each node has an address, the addresses of the main network being arranged in a hierarchical system, such that the address of a node will normally indicate the topological position of that node. In the present example, the addresses of the nodes are addressed according to the Internet Protocol, preferably version V6.

The mobile node 14 is configured to make a temporary connection with any one of a plurality of spaced apart attachment points 20 of the main network 12. Each attachment point will normally have a node, termed a foreign agent (FA) node 22 associated therewith (only one is shown for clarity). The foreign agent will normally issue the mobile node with a temporary address, which address is topologically related to that of the issuing foreign agent, (for example, the addresses may share a common prefix portion) such that packets addressed to the temporary or "care-of" address of the mobile node will be routed by the network to the foreign agent, which can then forward the packets to the mobile nodes.

The mobile node has an associated Home Agent (HA) node in the main network 12. The association between the mobile node and its home agent is formed at least in part by a permanent address allocated by the home agent to the mobile node, which the mobile node retains as it moves from one attachment point to another. The permanent or "home" address of the mobile node will be topologically related to the address of the home agent (for example by sharing a common prefix portion with the home agent address) such that packets from a caller node 26 (CN) addressed to the home address of the mobile node can be intercepted by the home agent. To allow the home agent to forward a packet from the caller node 26 towards the current attachment point of the mobile node, the home agent will store a mapping between the current care-of address of the mobile node and its home address, which mapping will be updated when the mobile node attaches to a new attachment point, that is, when the mobile node transmits a binding update to its home agent informing the home agent of its new care-of address.

The mobile node may be a router or a communications device on a vehicle, or otherwise the mobile node may be a portable device, such as a laptop computer, or another type of movable device. Preferably, the mobile node will have temporary connection means 32 for making a temporary connection 34 with an attachment point, for example a radio receiver and/or transmitter for making a radio connection 34, or a releasable electrical or optical connecter arrangement.

There are many circumstances in which authentication or other authorisation will be desirable before secure or reliable communication between two nodes is established. For example, the home agent for the mobile node may require proof of the identity of the mobile node before accepting a binding update, so as to reduce the risk of traffic intended for the mobile node being inadvertently forwarded by the home agent to a fraudulent node. The need for efficient security processes is particularly important in the case of traffic relating to a mobile node, since the topologically correct address of a mobile node is

temporary, that is, changeable as the mobile node moves. However, there are other situations where authorisation or authentication can be important: for example, the home agent may have a policy of only passing information to specified foreign agents, or likewise, a foreign agent may have a policy of only allowing mobile nodes to attach to it whose identity or other characteristics fall within a specified or predetermined category.

To reduce the risk of fraudulent authentication or authorisation, or other data transfer taking place, the main network 12 will normally include a certificate authority agent, here implemented as a certificate authority (CA) node 28. (It will be appreciated that the nodes CA, FA, MN, and HA will be implemented on hardware which will include at least one memory and at least one processor means, the hardware and software running thereon being located at a single node or otherwise being distributed over spaced apart hardware apparatus, for example over a plurality of nodes).

The certificate authority will normally employ a Public Key (PKI) encryption system. In such a system, also known as asymmetric key cryptography, an entity (such as a person or node) has associated therewith a pair of keys: a public key which is publicly accessible, for example by being distributed or being placed in a public directory; and, a private key; only accessible to the entity with which the pair of keys is associated. The pair of keys is mathematically linked, for example according to a known protocol developed by Diffie and Hellman. The mathematical function relating the two keys to one another is such that it is difficult, preferably unfeasible, to derive the private key from the related public key. This may be achieved for example by a function which requires an impractically large number to be factored in order to obtain the private key. Thus, a first person wishing to send an encrypted message for transmission to a second person can look up the public key associated with the first person in a public (and trusted) directory, and encrypt the message with the second person's public key. The second person can use their private key to decrypt the message. In this way, public key cryptography can be considered to be based on a one-way function, that is, a function which is significantly easier to perform in the forward direction than in the reverse direction. The public key provides an indication of an instance of the function, and the private key allows the function to be performed in the reverse direction.

In order to generate a certificate, the certificate authority will form a digital signature in association with the information content of the certificate. The digital signature will be the result of a mathematical algorithm, function, or other computation having as input parameters (a) the message content of the certificate, (b) the private key of the certificate authority. In particular, the digital signature will preferably be the result of

the encryption procedure using the private key of the certificate authority. A person wishing to read the certificate can then "de-crypt" the digital signature using the public key of the certificate authority (or equivalently, perform a function to generate signature information related to the encrypted signature). A checking algorithm can then be performed using the digital signature and the message content as input parameters to determine whether the received message corresponds to the digital signature, in particular whether the received message is the same as the transmitted message used to generate the digital signature. This is possible because for a given private key, the digital signature is (almost) unique to the message: that is, the likelihood of two different (non-identical messages) returning the same (even unencrypted) signature is very low. Furthermore, because the digital signature is encrypted, it is difficult for an unauthorised person to change the signature so as to reflect any changes that unauthorised person may have made to the message. In this way, the digital signature is indicative of the message content such that by performing predetermined respective functions on the received message content and the digital signature, and by comparing the results of those functions, it is possible to determine if the message content as received has been altered.

In more detail, to generate a certificate, the certificate authority will: perform a "hash" function on the certificate (message) content, or other function chosen such that there is a low likelihood of two different contents yielding the same result. The result of the hash function, known as the message digest, is then encrypted using the certificate authority's private key according to a PKI protocol. A recipient can then perform a recipient computation, related to that used to create the signature, the recipient computation function involving the message content, the received signature, and the sender's (here the certificate authority) signature. If the result is correct according to a predetermined mathematical relation, the signature can be deemed genuine, and the message content is unlikely to have been altered.

In more detail, a recipient can: "de-crypt" the signature using the public key, in order to obtain the message digest (or related information); perform the same hash function on the received message as was performed on the sent message; and, compare one message digest with the other. If these are the same, the signature is deemed genuine. When an entity (the issuee) is issued a certificate by the certificate authority, the message content of the certificate will normally contain at least some of the following items of information: name of issuing certificate authority; the public key of the certificate authority; an expiration date of the public key; the name or an identifier of the issuee; and, the public key of the issuee.

In addition, the message content will include location object identifier, or other geographical information, which geographical information is derived from a physical geographical position or an indication thereof. Examples of geographical information include; a latitude and longitude value (with optionally an altitude value); a map reference; a known place name; a street or road name; and, a street junction. Since geographical information is derived from a geographical location, it will be more reliable as an indication of position than other information such as an IP address, from which geographical position can sometimes be inferred.

A certificate 50 is illustrated in Figure 2, which shows: the message content 52; items of information such as geographical information 54; an identifier 56; and, the digital signature 58.

When the certificate authority issues a certificate to a node, the certificate authority will transmit the certificate to the requesting node over the network 12; that is, through one or more routing node 161 and links 18. The requesting node can then store the certificate in a memory, preferably in a local memory 30, such that the certificate can be transmitted to another node when needed, for example when information or services are required from that node.

Returning to the situation shown in Figure 1, the mobile node 14 will be issued with a certificate by the certificate authority 28. The certificate for the mobile node will normally have geographical information indicative of an area associated with the home agent's physical location, but the geographical information in the mobile nodes certificate may be other static geographical information, for example information relating to the owner's place of residence. In more detail, the geographical information will normally be in the form of a value associated with a location object identifier. Likewise, the home agent and foreign agent are also sent respective certificates by the certificate authority 28. The value for the location objection identifier for the home agent and foreign agent correspond to their respective physical locations as expressed in latitude and longitude. In this example, the value of the location object identifier for the mobile node corresponds to that of the home agent.

The steps involved in the attachment of the mobile node to the main network are shown schematically in Figure 3, in which information flow is indicated by arrows, increasing time being in the downward direction on the page. To begin the attachment process, the mobile node sends an initial registration packet to the foreign agent, which packet is "dropped" or read at the foreign agent. The initial packet triggers the start of an Internet Key Exchange (IKE) process for establishing a security association between the

mobile node and the foreign agent, in which process protocols are agreed. Once a secure association has been established, the mobile node may send encrypted traffic to the foreign agent.

As part of the registration process between the mobile node and the foreign agent, the mobile node will send its certificate to the foreign agent. The foreign agent can then: de-crypt the digital signature using the public key of the certificate authority, which public key the foreign agent may obtain from the certificate authority itself; perform a function on the content, which function (normally a hash function) has previously agreed (for example during the IKE procedure on the message); compare the result of the function with the decrypted signature; and, if the comparison indicate a match, treat the certificate as genuine. Assuming the certificate is genuine (or to ascertain or further verify that the certificate is genuine), the foreign agent can then extract the location object identifier from the message content of the certificate. The foreign agent may be configured to make a decision as to whether to grant or refuse foreign agent functionality to a mobile node in dependence on the geographical information in the mobile nodes certificate. In particular, the foreign agent may be configured to compare the location object identifier of the mobile node to information indicative of the foreign agent's own physical location information, which may be stored locally, and only grant access if the two items of location information have a specified characteristic in common. For example, access may only be granted if the location information of the mobile node and foreign agent indicate respective positions within the same specified geographical area or within a specified distance of one another. In this way, the foreign agent can be configured to only grant access to a mobile node which originates from the same geographical district or country as the foreign agent.

Assuming that the foreign agent can grant access, or provide other foreign agent functionality for the mobile node, the foreign agent will attempt to register with the home agent. To start this process, the foreign agent will transmit an initial registration packet, which packet is "dropped" at the home agent. This dropped packet initiates an IKE procedure as indicated in Figure 4. The home agent will receive a certificate from the foreign agent, and perform similar steps to those outlined above to determine whether the certificate is genuine. Again, the home agent may extract the location object identifier from the certificate of the foreign agent and may perform a comparison between the location object identifier and other stored geographical information. In particular, the home agent may compare the location object identifier against an expected location object identifier stored at a registry 36, which registry may store location object identifiers

respectively mapped to the identity of mobile nodes. Thus, the location object identifier in the certificate may serve to provide an additional security test in order to authenticate the foreign agent.

Once the mobile node is registered with the foreign agent, and the foreign agent is registered with the home agent, a secure association is formed on the one hand between the mobile node and the foreign agent, and on the other between the foreign agent and the home agent. Encrypted traffic can then be transmitted from the mobile node to the foreign agent, and then forwarded by the foreign agent to the home agent.

As the certificate is used for authentication in this secure association creation process, the location information contained in the certificate, and the associated IP address can be extracted and stored for future use. The home agent will normally have a security policy that grants or denies mobile IP services in dependence upon the location of the foreign agent. When a request for a mobile IP registration arrives at the home agent, the home agent may use the IP address of the request message to obtain the location of the care-of address for the mobile node. However, the certificate from the foreign agent will preferably be used to obtain the physical location of the foreign agent (or a confirmation thereof), as this is more reliable. Once the location of the foreign agent has been obtained, it can be compared against a policy associated with that location. If the mobile node is allowed mobile IP surfaces from the location of the foreign agent (the location of the mobile node being inferred from that of the foreign agent), then a registration-successful message will be sent back to the foreign agent, else a registration-unsuccessful message will be sent back.

It can be seen from the above that the location information in a certificate can be used by a node when deciding whether to provide information. In particular, the location information extracted from a certificate can be compared with stored location information, such that the decision as to whether surfaces are to be provided can be made at least in part in dependence upon the comparison between the extracted location information and the stored location information.

Further details on the implementation of one embodiment of the invention are provided below: the operating used is FreeBSD [FreeBSD]. The Internet Key Exchange (IKE) implementation comes from KAME [kame], the secure socket layer implementation comes from the openssl organisation [openssl] and the mobile IP implementation from Portland State University [psu]. The openssl code is used by the KAME IKE implementation. It is also assumed that security policy exists that state that secure communication must exist between the MN and the FA and also between the FA and the

HA. One stage is to introduce the location attribute into the certificate. This is done by introducing a new object identifier of type 2.5.5.4 [oid] and associating a value with this corresponding to the location expressed as x, y pair. It is also possible to include an altitude attribute as x, y, z where z represents the altitude although this was not done in this implementation. An example of such a certificate is shown in Figure 5 with the location object identifier and associated value shown. Another stage is to configure the IKE daemon, racoon [kane], to use certificates rather than pre-shared secrets. As shown schematically in Figure 3, the sending of the registration packet from the MN to FA initiates the generation of a security association between them. Lets focus on the creation of security associations between the FA and the HA since the creation of security associations between the FA and the MN is as described in standards [RFC2002]. Figure 4 shows the sequence of messages that occur in phase 1 of the creation of secure associations using IKE. Note that in Figure 4, the certificate payload has to be present since it may not be possible for the FA and the HA to get the certificate from other sources, say secure DNS. Where the diagram ends, phase 2 of the IKE processing can take place to create the IPsec secure association proper. It is intended to send the valid certificate to a local listener that will store the location and the IP address in a local file. The message from the IKE daemon is parsed. With regard to the processing of the certificate payload: the function saveFaLocation (currentLocation, ip_address) saves the location seen in the certificate and the associated ip address as a tuple in an ascii file. This file can then be read by other applications that require location dependent information. The home agent may have a policy for allowing mobility, which could be refined by defining bounded polygons for location, as in [RFC2009].

References

[RFC1712] http://www.ietf.org/rfc/rfc1712.txt

[geobytes] http://www.geobytes.com

[RFC2002] http://www.ief.org/rfc/rfc2002.txt

[newbury] http://www.newburynetworks.com

[RFC2401] http://www.ietf.org/rfc/rfc2401.txt

[FreeBSD] http://www.freebsd.org

[kame] http://www.kame.net

[openssl] http://www.openssl.org

[psu] http://www.cs.pdx.edu/research/SMN/index.hrml

[oid] http://www.alvestrand.no/objectid/

CLAIMS

1. A method of authorising data transfer to a mobile node, the method including the steps of: receiving a digital certificate from the mobile node, the digital certificate including a message body, a digital signature for verifying the content of the message body, and, geographical information derived from a physical location; performing a comparison between the geographical information of the certificate and a further item of geographical information; and, making an authorisation decision in dependence on the result of the comparison.

2. A method as claimed in claim 1, wherein the digital certificate is suitable for use in a public key encryption system

3. A method as claimed in claim 2, wherein the certificate is generated at a certificating node having a public key and a private key associated therewith, and wherein the signature is a function, at least in part, of the private key of the certificate node

4. A method as claimed in claim 2 or claim 3, including the step of verifying the authenticity of the digital certificate by performing a computation on at least part of certificate, the computation involving the public key associated with the certificate node.

5. A method as claimed any preceding claim, wherein the mobile node is configured to form a temporary attachment to an attachment point of a main network, and wherein the digital certificate is received at a network node in the main network.

6. A method as claimed in claim 5, wherein the attachment point has a forwarding node associated therewith for forwarding messages to and/or from the mobile node, and wherein the forwarding node has a digital certificate associated therewith, which certificate include geographical information derived from the physical location of the forwarding node, the method including the steps of: at the network node, receiving the digital certificate from the forwarding node; and, making an authorisation decision in dependence on the geographical information of the certificate from the forwarding node.

7. A method as claimed in claim 6, wherein the authorisation decision includes the step of inferring the location of the mobile node from the geographical information in the certificate of the forwarding node.

8. A method as claimed in any of claims 5 to 7, wherein the mobile node has a temporary address and a permanent address associated therewith.

9. A method as claimed in claim 8, wherein the temporary address of the mobile node is indicative of the topological position of the current point of attachment of the mobile node.

10. A method as claimed in claim 8 or claim 9, including the steps of: (i) intercepting packets addressed to the permanent address of the mobile node; and, (ii) forwarding the intercepted packets towards the temporary address of mobile node, at least one of steps (i) and (ii) being authorised in dependence on the result of the comparison.

11. A method as claimed in any preceding claim, including an authentication step.

12. A network node for authorising the transfer of data to a mobile node, wherein the network node is configured, in response to receiving a digital certificate from the mobile node, to read at least part of the digital certificate, the digital certificate including geographical information derived from a physical location, and wherein the network node is further configured to: perform a comparison between the geographical information of the certificate and a further item of geographical information; and, in dependence on the result of the comparison, make an authorisation decision.

13. A method of generating a digital certificate for use in an authorisation decision, the digital certificate being suitable for use in a public key cryptography protocol in which a message can be encrypted with a public key and decrypted with a private key, the digital certificate having a message body and a digital signature for verifying the message body, the method including the steps of: including geographical information in the message body, the geographical information being derived from a physical location; and, performing a computation involving the message body and a private key in order to form the digital signature.

14. A method of authorising a user, the method including the steps of: receiving a digital certificate from the user, the digital certificate including a message body, a digital signature for verifying the content of the message body, and, geographical information derived from a physical location; performing a comparison between the geographical information of the certificate and a further item of geographical information; and, making an authorisation decision in dependence on the result of the comparison.

ABSTRACT

Authorisation

The present invention relates to authentication, in particular to authentication using a digital certificate. The digital certificate includes geographical information derived from a physical location. A comparison between the geographical information of the certificate and a further item of geographical information can be performed. An authorisation decision can then be made in dependence on the result of the comparison.

Figure (1)

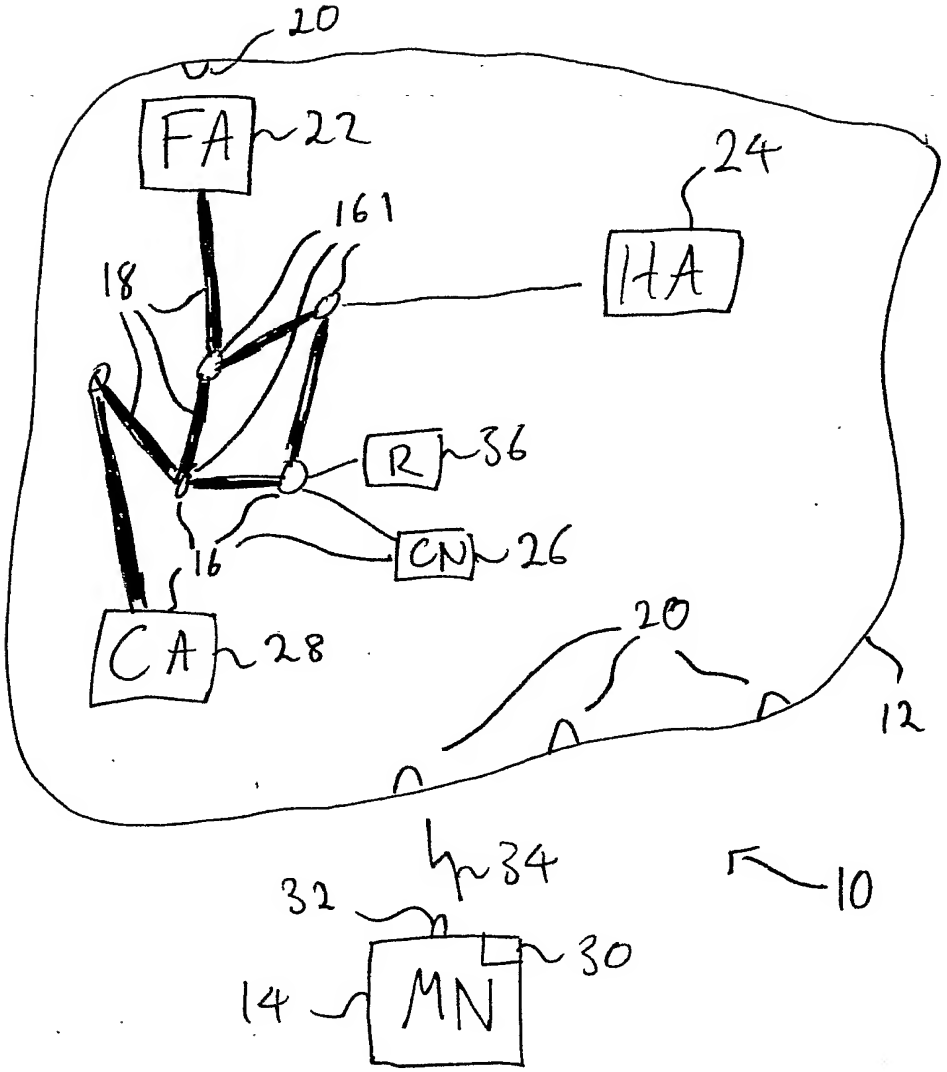

20
FA
22
24
161
HA
18
R
36
CN
26
16
CA
28
20
12
34
10
32
30
14
MN

Fig. 1

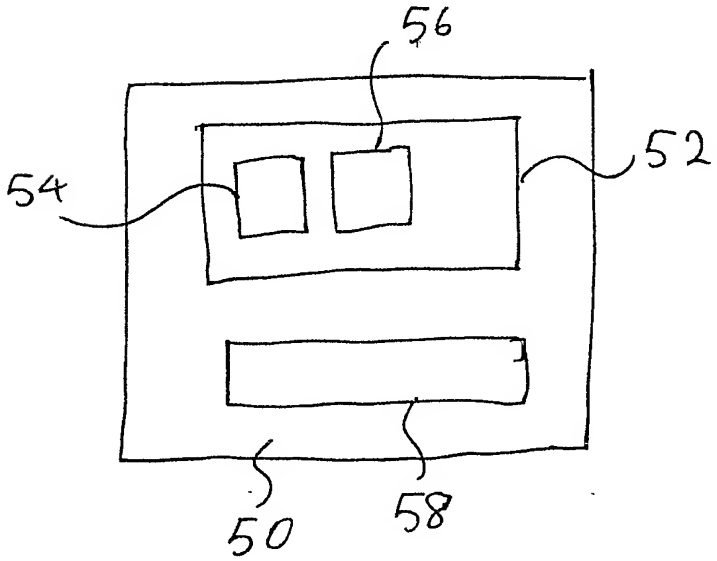
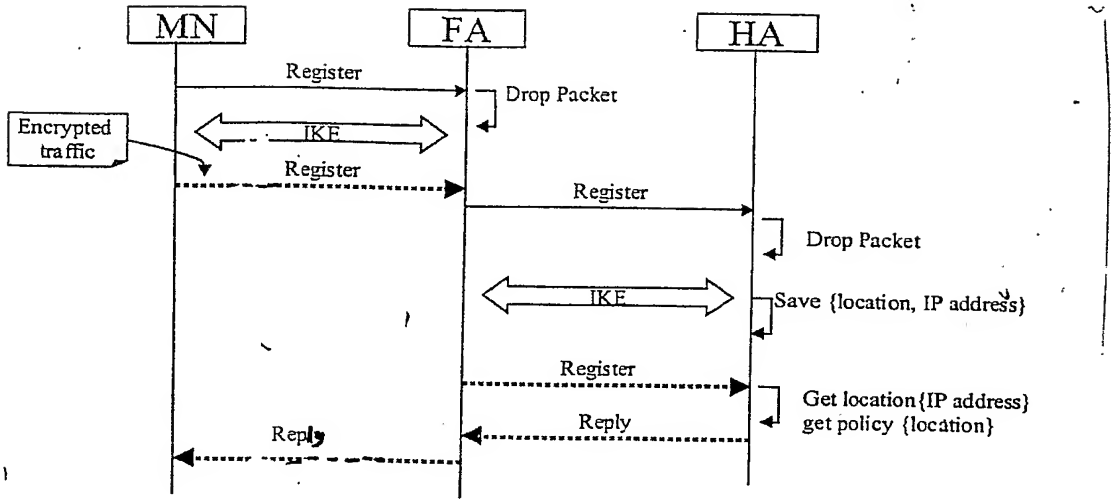

56
54
52
50
58

Fig. 2

Fig. 3


MN
FA
HA
Register
Drop Packet
Encrypted traffic
IKE
Register
Register
Drop Packet
IKE
Save {location, IP address}
Register
Get location{IP address}
get policy {location}
Reply
Reply

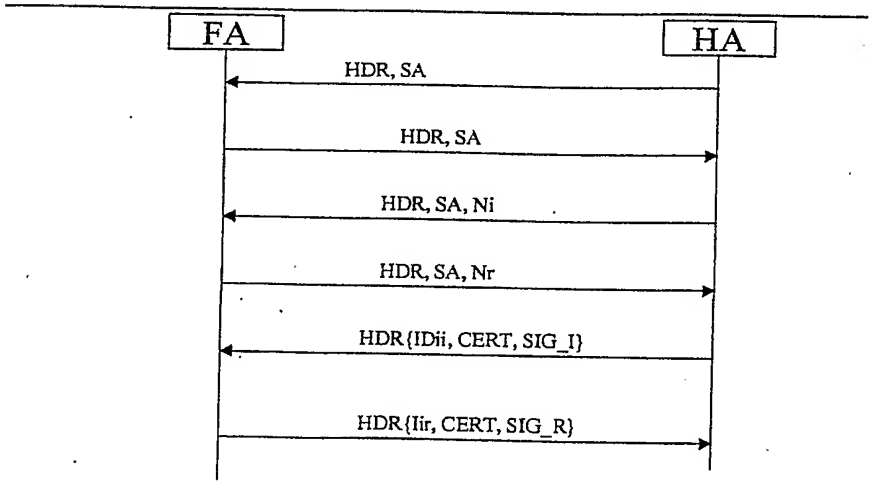

FA
HA
HDR, SA
HDR, SA
HDR, SA, Ni
HDR, SA, Nr
HDR{IDii, CERT, SIG_I}
HDR{Iir, CERT, SIG_R}

Fig. 4

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=UK, ST=Suffolk, L=Ipswich, O=BT, OU=BTexat,
CN=Administrator/Email=parminder.mudhar@bt.com/2.5.5.4=123456,123456
        Validity
            Not Before: Jul 11 13:14:30 2002 GMT
            Not After : Jul 11 13:14:30 2003 GMT
        Subject: C=UK, ST=Suffolk, O=BT, OU=BTexat,
CN=Singh/Email=parminder.mudhar@bt.com/2.5.5.4=123,345
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b5:09:9d:58:b5:4e:30:85:c4:68:c2:c3:53:13:
                    67:a4:fe:f0:2c:22:f2:de:65:e9:50:8e:4a:5f:93:
                    39:35:cf:10:f4:b9:1d:b5:b8:56:37:94:b5:a6:67:
                    70:e0:ee:e8:b5:0b:15:e0:01:c4:66:69:f4:05:72:
                    3a:1a:18:22:38:37:dd:ca:9e:9a:74:22:75:73:e6:
                    1e:6b:9d:1b:48:f6:d4:10:a7:cb:c1:c2:c7:b5:c9:
                    61:91:d0:0f:4a:b8:71:3c:cc:90:da:e9:74:fc:11:
                    4c:5b:43:51:f6:bc:06:57:5a:06:ed:9e:ed:8d:54:
                    65:62:ea:a9:7c:fa:88:01:cd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:

58:07:C0:76:5B:DF:BB:2B:23:92:3D:03:BF:EC:E8:F5:0C:32:39:5E
            X509v3 Authority Key Identifier:

keyid:B3:43:C9:28:B7:44:9E:5F:83:FB:D1:57:85:E0:EF:EB:9C:FF:DC:65
                DirName:/C=UK/ST=Suffolk/L=Ipswich/O=BT/OU=BTexat/
CN=Administrator/Email=parminder.mudhar@bt.com/
2.5.5.4=123456,123456
                serial:00

            X509v3 Subject Alternative Name:
                IP Address:192.168.7.3,
DNS:parminder_home.futures.bt.co.uk, email:parminder.mudhar@bt.com
    Signature Algorithm: md5WithRSAEncryption
        06:7f:b3:48:b5:93:e0:11:69:d7:cc:61:2e:64:e9:bd:01:8c:
        68:dc:a3:4b:be:e0:d2:21:17:98:86:21:9b:cb:73:3f:cf:2c:
        7e:1a:a4:ad:a5:e1:be:fd:0b:82:7e:85:f4:96:8a:65:3a:22:
        4a:fd:cd:64:91:3e:44:65:6c:24:80:01:77:f5:f4:4d:83:a2:
        d9:14:62:8e:71:99:74:28:3d:d1:45:51:90:95:19:a3:9a:e7:
        11:a8:74:50:8f:f0:b5:8d:97:71:6b:b7:7a:34:8e:00:59:f9:
        68:e8:f8:8f:76:2a:43:4b:c6:65:53:a6:c1:71:d3:18:8a:59:
        d5:cb:58:34:8f:40:8e:83:e3:35:b6:70:33:54:e4:d4:98:fe:
        d5:60:61:a8:64:9d:9d:8a:c9:18:a4:c1:e5:15:69:4e:57:19:
        18:71:d6:7e:37:5a:d0:29:ef:66:9e:19:cc:47:82:c5:20:ef:
        75:6b:0f:29:54:68:e2:2d:15:3c:cc:ae:43:af:98:df:18:55:
        a8:fb:5f:df:39:45:6c:00:f5:26:47:88:97:b6:63:74:de:ac:
        91:e4:a9:cb:e8:30:8b:64:30:09:42:c1:44:db:f9:49:38:92:
        f3:7a:c1:2b:1e:fa:4d:7f:38:e3:e0:76:32:84:c8:5a:cc:a5:
        73:11:f2:a8
```

Fig. 5